



DEPARTMENT OF THE ARMY  
HEADQUARTERS, JOINT READINESS TRAINING CENTER AND FORT POLK  
6661 WARRIOR TRAIL, BUILDING 350  
FORT POLK, LOUISIANA 71459-5339

AUG 07 2015

AFZX-IM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum G6-02 – Command Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

1. References.

- a. Army Regulation 340-21, The Army Privacy Program, 5 Jul 85.
- b. Memorandum, Department of Defense, Chief Information Officer, 18 Aug 06, subject: Department of Defense Guidance on Protecting Personally Identifiable Information (PII).
- c. DoD 5400.11-R, Department of Defense Privacy Program, 14 May 07.
- d. Message, ALARACT 50/2009, 26 Feb 09, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.
- e. Memorandum, Office of the Secretary of Defense, 5 Jun 09, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

2. Purpose. This standing operating procedure (SOP) will define PII and include specific procedures on how to protect and report the loss of PII.

3. Applicability. All Fort Polk units assigned or attached and Installation activities.

4. Definition. PII is defined as any information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life. Information includes, but is not limited to, education, financial transactions, medical history, criminal or employment history, and other information which can be used to distinguish or trace an individual's identity (such as, name, social security number, date and place of birth, mother's maiden name, biometric records, and so forth), including other personal information which is linked or linkable to an individual.

5. Policy. All personnel working on the Joint Readiness Training Center (JRTC) and Fort Polk have a direct responsibility to ensure Privacy Act information and PII are collected, maintained, used and disseminated only as authorized. Personnel are further

AFZX-IM

SUBJECT: Command Policy Memorandum G6-02 – Command Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

required to protect all PII data (hardcopy or electronic) from unauthorized use, access, disclosure, alteration or destruction. The PII will not be released to anyone who does not have an official need to know. Individuals who violate their responsibilities may be subject to adverse administrative, disciplinary, or other actions.

a. Assess. All records identified by data owners as containing PII will be assigned the appropriate impact category of high (500 + PII records) or moderate (any electronic record containing PII that is not identified as high impact). In addition, any high impact electronic PII record stored on a mobile computing device or portable media that is removed from the government (protected) workplace will be required to log and track these devices in accordance with (IAW) the established SOP using the form at enclosure 1.

b. Train. All users will complete the Department of Defense Cyber Awareness Challenge Training prior to accessing the Fort Polk NIPRNet.

c. Secure.

(1). The JRTC and Fort Polk approved data-at-rest (DAR) solution is the encrypting file system (EFS) folder. Other active measures in protecting PII are access control through common access card/public key infrastructure (CAC/PKI) and automatic screen lock-out enforcement. In addition, all personnel using JRTC and Fort Polk computer systems are responsible and directed to encrypt all email containing PII.

(2). The acceptable methods for disposal of paper records are tearing, burning, melting, chemical decomposing, pulping, pulverizing, shredding, or mutilating. Acceptable disposal methods for electronic records and media are overwriting, degaussing, disintegrating, pulverizing, burning, melting, incinerating, shredding or sanding. A risk assessment on all PII records will be evaluated for impact of loss or unauthorized disclosure and protected accordingly using the factors within enclosure 2.

d. Report. All breaches will be reported IAW the JRTC and Fort Polk Incident Response Plan, see enclosure 3:

- Within one (1) hour: incident reported to US-CERT (<http://www.us-cert.gov/>), S1/G1, S2/G2, S6/G6, Network Enterprise Center Information Assurance Manager, and the Installation Operations Center.

- Within 24 hours: incident reported to the JRTC and Fort Polk Freedom of Information Act/Privacy Act office at 531-1612.

AFZX-IM

SUBJECT: Command Policy Memorandum G6-02 – Command Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

- Within 48 hours: incident reported to Army leadership at [pii.reporting@us.army.mil](mailto:pii.reporting@us.army.mil).

e. Notification of Personnel Affected by PII Loss. When PII is lost, stolen, or compromised, "Notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered, and the identities of the individuals are ascertained." A sample letter to affected individuals can be accessed at: <https://www.rmda.army.mil/organization/pa-guidance.shtml> and is also at enclosure 4. All personnel must be knowledgeable of the procedures for reporting the loss of PII. The format to report this information is contained within enclosure 3.

f. Reimburse. A fine of up to \$5,000.00 can be imposed for failure to protect PII.

6. This policy supersedes and rescinds all previous policies and SOPs on this subject matter.

7. The point of contact for this SOP is the ACoS G6 at commercial (337) 531-5995 or DSN 863-5995.

4 Encls

1. High Impact PII Log Form
2. Risk Assessment Model
3. DD Form 2959 (PII Breach Report)
4. Sample Letters



TIMOTHY P. MCGUIRE  
Brigadier General, USA  
Commanding

DISTRIBUTION:

A+



**FORSCOM REPORTING PROCEDURES FOR THE NOTIFICATION OF  
PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH OR COMPROMISE  
INCIDENT**

1. Upon discovery of the loss, theft or compromise of PII, contact the FORSCOM Privacy Act (PA) Officer immediately. The PA Officer will assist with determining if a valid breach has occurred, reporting the incident thru proper channels and notifying the individual.
2. Incidents must be reported within one hour to the U.S. Computer Emergency Readiness Team ([www.uscert.gov](http://www.uscert.gov)), the U.S. Army PII Incident Reporting System ([www.rmda.army.mil](http://www.rmda.army.mil)) within 24 hours, and the Army Leadership at [PII.reporting@us.army.mil](mailto:PII.reporting@us.army.mil). In some instances, the credit card company, local law enforcement, and the public affairs office may require notification. The PA Officer will assist with this additional notification requirement.
3. At a minimum, the PII Incident Report will contain the following information:
  - a. Organization involved:
  - b. Date of Incident and estimated number of individuals impacted:
  - c. Brief description of the incident (either suspected or confirmed);  
circumstances of the breach; information lost or compromised:
  - d. Point of contact (name, telephone number, and email) of individual  
who discovered the breach or compromise:
4. In the event of a breach, a PII risk assessment will be performed to evaluate the impact of loss or unauthorized disclosure using Appendix A and Table 1 outlined in the DoD Memorandum, Subject: Safeguarding Against and Responding to the Breach of PII dated 05 June 2009. Both Appendix A and Table 1 are located on the FCCS Portal.
5. The FORSCOM PA Officer is Ms. Gayla Uslu can be reached at (404) 464-6238 or [gayla.uslu@conus.army.mil](mailto:gayla.uslu@conus.army.mil).

## BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT

<b>INITIAL REPORT</b>	<b>UPDATED REPORT</b>	<b>AFTER ACTION REPORT</b>
Date: (MM/DD/YYYY)		
Date: (MM/DD/YYYY)		
Date: (MM/DD/YYYY)		
<b>1. GENERAL INFORMATION</b>		
a. DATE OF BREACH (MM/DD/YYYY)	b. DATE BREACH DISCOVERED (MM/DD/YYYY)	c. DATE REPORTED TO US-CERT (MM/DD/YYYY)
d. US-CERT NUMBER		
e. COMPONENT INTERNAL TRACKING NUMBER (If applicable)	f. BREACH INVOLVED (Click to select)	g. TYPE OF BREACH (Click to select)
h. CAUSE OF BREACH (Click to select)		
i. COMPONENT (Click to select)		j. OFFICE NAME
POINT OF CONTACT FOR FURTHER INFORMATION:		
k. FIRST NAME	l. LAST NAME	m. RANK/GRADE AND TITLE
n. DUTY E-MAIL ADDRESS		o. DUTY TELEPHONE NUMBER
MAILING ADDRESS:		
p. ADDRESS		q. CITY
		r. STATE
		s. ZIP CODE
2.a. DESCRIPTION OF BREACH (Up to 150 words, bullet format acceptable). NOTE: Do NOT include PII or Classified Information.		
2.b. ACTIONS TAKEN IN RESPONSE TO BREACH, TO INCLUDE ACTIONS TAKEN TO PREVENT RECURRENCE AND LESSONS LEARNED (Up to 150 words, bullet format acceptable). NOTE: Do NOT include PII or Classified Information.		

<b>3.a. NUMBER OF INDIVIDUALS AFFECTED</b> (1) Contractors <input type="checkbox"/> (2) DoD Civilian Personnel <input type="checkbox"/> (3) Military Active Duty Personnel <input type="checkbox"/> (4) Military Family Members <input type="checkbox"/> (5) Military Reservists <input type="checkbox"/> (6) Military Retirees <input type="checkbox"/> (7) National Guard <input type="checkbox"/> (8) Other (Specify): <input type="text"/>		<b>b. WERE AFFECTED INDIVIDUALS NOTIFIED?</b> Yes <input type="checkbox"/> No <input type="checkbox"/> (2) If Yes, notification date (MM/DD/YYYY) <input type="text"/> (4) If notification will not be made, explain why, or if number of individuals notified differs from total number of individuals affected, explain why: <input type="text"/> (5) If applicable, was credit monitoring offered? Yes <input type="checkbox"/> No <input type="checkbox"/>		(1) If Yes, were they notified within 10 working days? Yes <input type="checkbox"/> No <input type="checkbox"/> (3) If Yes, number of individuals notified: <input type="text"/> (6) If Yes, number of individuals offered credit monitoring: <input type="text"/>	
<b>4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH (X all types that apply)</b>					
<input type="checkbox"/> (1) Names <input type="checkbox"/> (2) Social Security Numbers <input type="checkbox"/> (3) Dates of Birth <input type="checkbox"/> (4) Protected Health Information (PHI) <input type="checkbox"/> (5) Personal e-mail addresses <input type="checkbox"/> (6) Personal home addresses		<input type="checkbox"/> (7) Passwords <input type="checkbox"/> (8) Financial Information* <input type="checkbox"/> (9) Other (Specify): <input type="text"/>		*If Financial Information was selected, provide additional detail: <input type="checkbox"/> (a) Personal financial information <input type="checkbox"/> (b) Government credit card If yes, was issuing bank notified? Yes <input type="checkbox"/> No <input type="checkbox"/> <input type="checkbox"/> (c) Other (Specify): <input type="text"/>	
<b>5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH</b>					
<b>a. PAPER DOCUMENTS/RECORDS (If selected, provide additional detail)</b> <input type="checkbox"/> (1) Paper documents faxed <input type="checkbox"/> (2) Paper documents/records mailed <input type="checkbox"/> (3) Paper documents/records disposed of improperly <input type="checkbox"/> (4) Unauthorized disclosure of paper documents/records <input type="checkbox"/> (5) Other (Specify): <input type="text"/>			<b>b. EQUIPMENT (If selected, provide additional detail)</b> <input type="checkbox"/> (1) Location of equipment <input type="checkbox"/> (2) Equipment disposed of improperly <input type="checkbox"/> (3) Equipment owner <input type="checkbox"/> (4) Government equipment Data At Rest (DAR) encrypted <input type="checkbox"/> (5) Government equipment password or PKI/CAC protected <input type="checkbox"/> (6) Personal equipment password protected or commercially encrypted		
<b>c. IF EQUIPMENT, NUMBER OF ITEMS INVOLVED</b>					
<input type="checkbox"/> (1) Laptop/Tablet <input type="checkbox"/> (2) Cell phone <input type="checkbox"/> (3) Personal Digital Assistant		<input type="checkbox"/> (4) MP3 player <input type="checkbox"/> (5) Printer/Copier/Fax/Scanner <input type="checkbox"/> (6) Desktop computer		<input type="checkbox"/> (7) Flash drive/USB stick/other removable media (If Other, Specify): <input type="text"/> <input type="checkbox"/> (8) External hard drive <input type="checkbox"/> (9) Other	
<b>d. EMAIL (If selected, provide additional detail)</b> <input type="checkbox"/> (1) Email encrypted <input type="checkbox"/> (2) Email was sent to commercial account (i.e., .com or .net) <input type="checkbox"/> (3) Email was sent to other Federal agency <input type="checkbox"/> (4) Email recipients had a need to know			<b>e. INFO DISSEMINATION (If selected, provide additional detail)</b> <input type="checkbox"/> (1) Information was posted to the Internet <input type="checkbox"/> (2) Information was posted to an intranet (e.g., SharePoint or Portal) <input type="checkbox"/> (3) Information was accessible to others without need-to-know on a share drive <input type="checkbox"/> (4) Information was disclosed verbally <input type="checkbox"/> (5) Recipients had a need to know		
<b>f. OTHER (Specify):</b> <input type="text"/>					
<b>6.a. TYPE OF INQUIRY (If applicable) (Click to select) (If Other, specify)</b> <input type="text"/>				<b>b. IMPACT DETERMINATION (for Component Privacy Official or designee use only) (X one)</b> <input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	
<b>c. ADDITIONAL NOTES (Up to 150 words, bullet format acceptable) NOTE: Do NOT include PII or Classified Information.</b> <div style="height: 150px; border: 1px solid black;"></div>					

**INSTRUCTIONS FOR COMPLETING DD FORM 2959,  
BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT**

Select Initial, Updated, or After Action Report and enter the date.

**1. GENERAL INFORMATION.**

- a. Date of Breach. Enter the date the breach occurred. If the specific date cannot be determined, enter an estimated date and provide further explanation in the notes section of the report.
- b. Date Breach Discovered. Enter the date the breach was initially discovered by a DoD employee, military member, or DoD contractor.
- c. Date reported to US-CERT. Breaches must be reported to US-CERT within 1 hour of discovery. Enter the date reported to US-CERT.
- d. US-CERT Number. Enter the number assigned by US-CERT when the breach was reported.
- e. Component Internal Tracking Number (if applicable). If your component uses an internal tracking number, enter the number assigned.
- f. Breach Involved (click to select). Select from the drop-down list - Email, Info Dissemination, Paper Records, or Equipment.
- g. Type of Breach (click to select). Select from the drop-down list - Theft, Loss, or Compromise.
- h. Cause of Breach (click to select). Select from the drop-down list the predominate cause of the breach - Theft, Failure to Follow Policy, Computer Hacking, Social Engineering, Equipment Malfunction, Failure to Safeguard Government Equipment or Information, Improper Security Settings, or Other.
- i. - j. Component. Select from the drop-down list. After you select your Component, enter the Office/Name in block 1.j (i.e., if "OSD/JS" is the Component selected, an example of the Office would be "TMA").
- k. - s. Point of Contact for Further Information. Enter the requested information for the person to be contacted if DPCLC requires additional details regarding the breach.

**2.a. DESCRIPTION OF BREACH** (Up to 150 words, bullet format acceptable). Note: Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss or compromise of PII as currently known, including:

- the description of the parties involved in the breach;
- the physical or electronic storage location of the data at risk;
- if steps were immediately taken to contain the breach;
- whether the breach is an isolated incident or a systemic problem;
- who conducted the investigation of the breach; and
- any other pertinent information.

**b. ACTIONS TAKEN IN RESPONSE TO BREACH, TO INCLUDE ACTIONS TAKEN TO PREVENT RECURRENCE AND LESSONS LEARNED** (Up to 150 words, bullet format acceptable). Note: Do not include PII or classified information. Summarize steps taken to mitigate actual or potential harm to the individuals affected and the organization. For example, training, disciplinary action, policy development or modification, information systems modifications. List any findings resulting from the investigation of the breach.

**3.a. NUMBER OF INDIVIDUALS AFFECTED.** For each category of individuals listed, enter the number of individuals affected by the breach. Do not include an individual in more than one category.

- b. Were affected individuals notified? Check box "Yes" or "No". If the individuals affected will not receive a formal notification letter about the breach, select "No" and enter an explanation of why the Component determined notification was not necessary in 3.b.(4). If additional space is needed for this justification, continue text in 6.c., Additional Notes.
- (1) If affected individuals were notified, were they notified within 10 working days? Check "Yes" or "No".
- (2) If the affected individuals will be notified of the breach, provide the date the notification letters will be sent.
- (3) - (4) If "Yes", list the number of individuals notified. If the number of individuals notified differs from total number of individuals affected, explain why in 3.b.(4).
- (5) Was credit monitoring offered? Select "Yes" or "No".
- Note: This is a risk of harm based decision to be made by the DoD Component.
- (6) If "Yes", enter the number of individuals offered credit monitoring.

**4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH.** Select all that apply. If Financial Information is selected, provide additional details.

**5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH.** Check at least one box from the options given. If you need to use the "Other" option, you must specify other equipment involved.

- a. Paper Documents/Records. If you choose Paper Documents/Records, answer each associated question by selecting from the drop-down options.
- b. - c. Equipment. If you choose Equipment, answer the associated questions by selecting from the drop-down options. Enter a number in the empty field indicating how many pieces of each type of equipment were involved in the breach. If "Other", you will need to specify what type of equipment was involved.
- d. - e. Email and Info Dissemination. If Email or Info Dissemination is selected, choose either "Yes" or "No" for all of the questions.

**6.a. TYPE OF INQUIRY.** Select the type of inquiry conducted as a result of the breach. If the inquiry type is "Other", please describe.

b. Impact Determination. (Component Privacy Official or designee use only.) Select one: What is the overall risk level associated with this breach? Risk is determined by considering the likelihood that the PII can be accessed by an unauthorized person and assessing the impact to the organization and individual if the PII is misused.

c. Additional Notes. This field can be used to convey additional information.



REPLY TO  
ATTENTION OF:

[Office]

Name  
Street Address  
Apartment 3  
Anywhere, NY 00000-0000

Dear [Name]:

On [date] personal information pertaining to you maintained by the Department of [Army/Defense], [contractor company name if applicable] [was/may have been] [stolen/lost/compromised/ publicly released]. The information was contained on a [laptop/website/email/document] and contained your [describe all data elements compromised – name, social security number, home address, date of birth, personal email address, home telephone number, etc.].

[Provide a detailed description of what took place, omitting names of personnel involved and details that could affect ongoing investigations.] STYLE EXAMPLE: An Army laptop computer was stolen from the parked car of an Army recruiter in New Orleans, Louisiana after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 members of the public who were potential recruiting prospects.

The [theft/loss/compromise/release] was immediately reported to [name(s) of local, Army, DoD law enforcement agency(s)] who [is/are] now conducting an [joint] inquiry into the matter. [If a theft, indicate whether we believe the data or the equipment was the target of the theft.] [If applicable, indicate whether the data was password protected, encrypted, etc.] [If a website posting, indicate the information was immediately removed upon discovery]. Although we cannot say with certainty, based on these circumstances we believe the probability is [low, moderate, high] that the information will be acquired and used for an unlawful purpose. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission at its Web site at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>. The FTC urges that you immediately place an initial fraud alert on your credit file. The fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card is changed. The site also provides other valuable information that can be taken now or in the future if problems should develop. The Social Security Administration has a toll-free number, 1-800-772-1213, and additional contact information is found on their web site <http://www.ssa.gov/reach.htm>. You may also want to monitor your credit reports by contacting: Transunion <http://www.transunion.com/index.jsp>; Equifax <http://www.equifax.com/>; and Experian <http://www.experian.com/>.

The above listed actions are not an exhaustive list of protective measures you may choose to take. There may be additional organizations or people with whom you may wish to consult, depending on your circumstances.

[If applicable: The Army is providing credit monitoring services to you for a period of [number] months. This service is being provided at no cost to you. Provide details of the credit monitoring conditions, such as what company, for which credit bureaus, points of contact, etc.]

The Army takes this loss very seriously and is reviewing current policies and practices with a view of determining what can or must be changed to preclude a similar occurrence in the future. [Indicate any special steps being taken]. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you. Should you have any questions, please call [POC name, email and phone number].

Sincerely,

[Signature block of Director level or higher official]

## SAMPLE WRITING STYLE: THEFT OF LAPTOP

On April 12, 2007, an Army laptop computer was stolen from the parked car of an Army recruiter in New Orleans, Louisiana after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 members of the public who were potential recruiting prospects. The compromised information included the name, social security number, home address, date of birth, school, personal email address, and home telephone number of recruiting prospects. The theft was immediately reported to the New Orleans Police Department and to the U.S. Army Criminal Investigation Command, who are now conducting inquiries into the theft.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information on the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.